

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/CN04/001557

International filing date: 29 December 2004 (29.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: CN
Number: 200410000042.1
Filing date: 05 January 2004 (05.01.2004)

Date of receipt at the International Bureau: 09 March 2005 (09.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

证 明

本证明之附件是向本局提交的下列专利申请副本

申 请 日： 2004. 01. 05

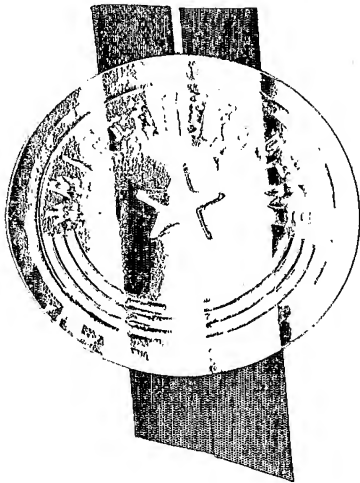
申 请 号： 2004100000421

申 请 类 别： 发明

发明创造名称： 一种网络安全系统和方法

申 请 人： 华为技术有限公司

发明人或设计人： 陈显义、危自强、吴娇黎、王恩奎、徐凌峰



中华人民共和国
国家知识产权局局长

王 景 川

2005 年 1 月 13 日

权 利 要 求 书

1. 一种网络安全系统, 包括设置在内部网络和外部网络之间的防火墙, 所述防火墙包括设在防火墙内侧的第一端口和设在防火墙外侧的第二端口, 其特征在于: 还包括设置在防火墙和外部网络之间的可信节点, 所述可信节点包括用于收敛可信节点与第二端口之间传送的数据的媒体流接收端口。

2. 根据权利要求 1 所述的网络安全系统, 其特征在于: 所述可信节点还包控制单元, 用于控制各单元的工作; 数据转发单元, 用于转发内部网络和外部网络之间传送的数据; 信令通道选择单元, 用于选择数据传送时信令传送的通道; 呼叫通道选择单元, 用于选择可信节点中一适合的媒体流接收端口以与内部网络通信。

3. 根据权利要求 1 或 2 所述的网络安全系统, 其特征在于: 所述可信节点支持 H323 协议。

4. 根据权利要求 1 或 2 所述的网络安全系统, 其特征在于: 所述信令通道选择单元采用 Q931 通道传送信令。

5. 一种网络安全方法, 利用一种网络安全系统实现内部网络与外部网络之间的安全通信, 所述的系统包括设置于内部网络与外部网络之间的防火墙、设置于防火墙两侧的第一端口及第二端口及设置于防火墙与外部网络间的可信节点, 所述的可信节点包括有媒体流接收端口, 其特征在于, 所述的方法包括步骤:

- 1) 通过所述可信节点建立内部网络和外部网络之间的呼叫连接;
- 2) 在可信节点中选择一适合的媒体流接收端口, 以与内部网络通信;
- 3) 可信节点转发内部网络与外部网络间传送的数据, 同时利用媒体流接收端口实现在可信节点和第二端口之间传送的数据的收敛。

6. 根据权利要求 5 所述的网络安全方法, 其特征在于: 步骤 2) 具体包括步骤:

- 21)、内部网络向可信节点发出打开逻辑通道信令;
- 22)、可信节点将选定的媒体流接收端口通知内部网络;
- 23)、可信节点向外部网络发送打开逻辑通道信令, 建立相应的通道。



7. 根据权利要求 5 所述的网络安全方法, 其特征在于: 步骤 3) 具体包括步骤:

- 31)、所述可信节点的媒体流接收端口接收所有来自内部网络的数据;
- 32)、所述可信节点将所述数据转发至外部网络;
- 33)、所述可信节点的媒体流端口将外部网络发出的数据转发至内部网络。

8. 根据权利要求 5 所述的网络安全方法, 其特征在于: 步骤 1) 包括选择 Q931 通道传送信令的步骤。

9. 根据权利要求 5 至 8 任一项所述的网络安全方法, 其特征在于: 步骤 1) 还包括当在多个可信节点之间实现负载均衡的步骤。



说明书

一种网络安全系统和方法

技术领域

本发明涉及一种电子或通信领域的网络安全技术，尤指一种网络安全系统和方法。

背景技术

近年来，伴随着互联网用户数量的不断增长，基于 IP (Internet Protocol, 互联网协议) 网络的业务应用越来越多，但 IP 技术在成为构筑网络应用主流技术的同时，其与生俱来的简单和开放的本质特征并没有得到根本性的改变，这就为网络安全问题的出现留下了隐患，尤其是对于企业用户，由于上述安全隐患的存在，就使得商业机密在网上进行传送时很可能因为黑客们的恶意攻击而变成没有安全性的数据，这种情况的存在对银行、保险、证券等金融企业用户更是严重。

因此，保证数据传送的安全就成了企业急需要解决的问题。目前，为保证用户内部网络（小区、企业网等）不受外部网络的攻击，通常的做法是在内部网络的出口设置防火墙，以使内部与外部隔绝，保证安全性。但上述方法在应用于视讯通信（特别是多点的视讯通信）时，由于需要在防火墙上开放很多端口，而且需要与很多外界节点（不安全节点）通信，所以会降低防火墙的隔离作用，进而导致内部网络被攻击的危险性增加。

为了克服上述视讯通信中的安全隐患，现有技术中通常采用如下的技术方案：

请参考图 1，为一种防火墙安全系统，具体方案为：在内部网络 10 和外部网络 20 之间设置防火墙 30，同时在防火墙 30 内外分别设置网络代理 41 和 42。所有内部网络 10 到外部网络 20 的视频码流都先经过网络代理 41，由网络代理 41 将码流、信令复用后发给防火墙 30 外的网络代理 42，网络代理 42 将收到的码流解复用后再发送给相应的节点。同理，外部网络 20 的码流、信令也都先经过网络代理 42，由网络代理 42 复用后发给网络代理 41。但是，该现有技术存在一些缺陷：



1. 由于在传送过程中涉及到两次码流的复用和解复用，要有一个将多个节点的数据拼接并插入标识的过程，同时还要有一个对复用数据根据标识拆成各个节点数据的过程，这样的过程需要时间，增加了处理的时延，从而对实时性要求很高的服务请求，例如视讯通信造成很大影响。同时数据经过了两个网络代理 41 和 42，也增加了时延。
2. 由于在系统中引入两个网络代理 41 和 42，使得整个系统的成本大为增加。

发明内容

本发明提供一种网络安全系统和方法，以解决现有技术中存在的数据传送时延问题。

为解决上述问题，本发明提供如下技术方案：

一种网络安全系统，包括设置在内部网络和外部网络之间的防火墙，所述防火墙包括设在防火墙内侧的第一端口和设在防火墙外侧的第二端口，该网络安全系统还包括设置在防火墙和外部网络之间的可信节点，所述可信节点包括用于收敛可信节点与第二端口之间传送的数据的媒体流接收端口。

一种网络安全方法，利用一种网络安全系统实现内部网络与外部网络之间的安全通信，所述的系统包括设置于内部网络与外部网络之间的防火墙、设置于防火墙两侧的第一端口及第二端口及设置于防火墙与外部网络间的可信节点，所述的可信节点包括有媒体流接收端口，所述的方法包括步骤：通过所述可信节点建立内部网络和外部网络之间的呼叫连接，选择可信节点与内部网络通信的媒体流接收端口，可信节点转发内外部网络之间传送的数据，同时利用媒体流接收端口实现在可信节点和第二端口之间传送的数据的收敛。

相对于现有技术，本发明的有益效果是：

1. 由于本发明在防火墙和外部网络之间引入可信节点，所有内部与外部网络之间的数据传送都先经过可信节点，而且由于在防火墙外侧开设对应于可信节点的第二端口，可信节点和内部网络的数据传送经过同一媒体流接收端口实现收敛，使得可信节点只对数据做转发处理，从而避免了现有技术对数据复用、解复用的过程，基本不增加数据流的



时延, 而且由于只经过了一个设备即可信节点, 时延相对现有技术也会较小。

2. 所有内部网络的节点都与可信节点发生信息交换, 在防火墙上可以对可信节点做更严格的限制, 而且可信节点与内部节点实现了端口的收敛, 大大减少防火墙所需要打开的传输层端口数, 可以简化配置, 保证了内外网络的隔离, 增强网络安全性。
3. 由于只引入可信节点, 其成本相对现有技术有所降低。
4. 可以根据需要同时部署多个可信节点, 实现负载均衡。扩展性非常好。

附图说明

图 1 是现有技术网络安全系统的框图;

图 2 是本发明网络安全系统的原理图;

图 3 是本发明网络安全方法的流程图;

图 4 是本发明网络安全系统的组网图;

图 5 是图 4 中所示可信节点之框图;

图 6 是本发明网络安全方法建立呼叫的流程图;

图 7 是本发明网络安全方法进行数据传送的流程图。

具体实施方式

请参阅图 2, 是本发明网络安全系统的原理图。该网络安全系统 100 支持 H323 协议, H323 协议是 ITU (International Telecommunication Union, 国际电信联盟) 多媒体通信系列标准 H.32x 的一部份, 该协议使得在现有通信网络上进行视频会议成为可能, 为现有的分组网络 (如 IP 网络) 提供多媒体通信标准。若和其它的 IP 技术如 IETF (Internet Engineering Task Force, 国际互联网工程师作业规程) 的资源预留协议 (RSVP) 相结合, 就可以实现 IP 网络的多媒体通信。H.323 协议中, 实时传送协议采用了 IETF 的 RTP (Real-time Transport Protocol)。

该网络安全系统 100 位于内部网络 810 和外部网络 820 之间, 隔离内部网络 810 和外部网络 820, 同时提供内部网络 810 和外部网络 820 之间的数据传送通道。该网络安全系统 100 包括防火墙 110 和可信节点 120, 其中防火墙 110 设置在内部网络 810 和外部网络 820 之间, 可信节点 120 位于防火墙 110 和外



部网络 820 之间。

该防火墙 110 可以是现有已知的各种类型的防火墙,主要起隔绝内部网络 810 和外部网络 820 的作用。为了进行内外部网络之间的数据交换,开展必要的网络应用,例如视讯通信,在防火墙 110 的内侧(即防火墙 110 与内部网络 810 之间)开设多个第一端口 111,同时在防火墙 110 的外侧(即防火墙 110 与外部网络 820 之间)开设第二端口 112,该第二端口 112 对应于可信节点 120。

该可信节点 120 的含义是指该节点是可以信任的,该节点发送的数据不会对内部网络 810 及用户的网络、机器造成伤害,其选取依据不同的应用场合而由内部网络管理者确认,可信节点 120 具有媒体流接收端口 129,并且可信节点 120 和内部网络 810 的数据传送经过媒体流接收端口 129 实现收敛。

请一并参阅图 2 和图 3,本发明网络安全方法利用所述网络安全系统 100 实现内部网络 810 与外部网络 820 之间的安全通信,包括:通过可信节点 120 建立内部网络 810 和外部网络 820 之间的呼叫连接的步骤 S1;选择媒体流接收端口 129 的步骤 S2;可信节点 120 转发内外部网络之间传送的数据的步骤 S3。其中,所有来自内部网络 810 的信令往可信节点 120 同一端口发送,信令端口的收敛可以通过 H323 中的 H245 隧道来完成。可信节点 120 通过 H245 信令中打开逻辑通道时选择与内部网络 810 通信的媒体流接收端口 129,其中防火墙 110 的第二端口 112 对应于可信节点 120 的媒体流接收端口 129,并且告知内部网络 810 相同的媒体流接收端口 129,因为码流往可信节点 120 同一端口即媒体流接收端口 129 发送,所以可信节点 120 和内部网络 810 的数据传送经媒体流接收端口 129 实现收敛。可信节点 120 再将信令、码流转发给外部网络 820。同理,可信节点 120 接收来自外部网络 820 的信令、码流并沿着该发送通道转发给内部网络 810。

请参阅图 4,是本发明网络安全系统的实施方式。其中,内部网络 810 包括多个内部节点,如终端 811、多点控制单元 812 和网关 813,外部网络 820 也包括终端 821、多点控制单元 822 和网关 823 等多个外部节点。防火墙 110 (参见图 2)和可信节点 120 隔离内部网络 810 和外部网络 820,同时提供内部网络 810 和外部网络 820 之间的数据传送通道,在此,防火墙 110 相对可信



节点 110 来说是透明的。

该网络安全系统 100 中还具有网守 400，网络中的内部节点 811-813、外部节点 821-823 和可信节点 120 都注册在网守 400 上。网守 400 的功能是向网络中各节点提供呼叫控制服务，其必须提供以下四种服务：地址翻译、带宽控制、许可控制与区域管理功能，另外，带宽管理、呼叫鉴权、呼叫控制信令和呼叫管理等为网守 400 的可选功能。虽然从逻辑上，网守 400 和网络中各节点是分离的，但是生产商可以将网守 400 的功能融入终端 811 及 821、多点控制单元 812 及 822 和网关 813 及 823 等物理设备中。由网守 400 管理的所有终端 811 及 821、多点控制单元 812 及 822 和网关 813 及 823 的集合称之为域。

请一并参阅图 5，该可信节点 120 还包括控制单元 121、数据转发单元 122、信令通道选择单元 123 和呼叫通道选择单元 124，其中控制单元 121 控制其他单元，数据转发单元 122 转发内部网络 810 和外部网络 820 之间传送的数据，信令通道选择单元 122 采用 Q931 通道传送信令，呼叫通道选择单元 124 选择内部网络 810 和外部网络 820 之间数据传送的通道，即选择可信节点 120 与内部网络 810 通信用媒体流接收端口 129。该可信节点 120 支持 H323 协议，其中采用 RAS（注册、许可、状态）完成可信节点 120 在网守 400 上的注册；采用 H.225.0 协议建立呼叫模型；采用 H.245 协议（多媒体通信控制协议）提供端到端信令，以保证内部网络 810 和外部网络之间的正常通信 820。H.245 协议定义了请求、应答、信令和指示四种信息，通过各种节点间进行通信能力协商，打开/关闭逻辑信道，发送命令或指示等操作，完成对通信的控制。

请一并参阅图 4、图 5 和图 6，以内部终端 811 与外部终端 821 之间的视讯通信为例说明本发明网络安全方法建立呼叫的流程，其包括：

1. 终端 811 向其注册的网守 400 发出 ARQ（Admission Request）请求，进行用户接入认证的步骤 601；
2. 网守 400 解析该 ARQ 请求的步骤 602，判断是否合法，如果不合法，则执行步骤 603，返回 ARJ（Admission Reject）信息，该信息一般包含失败原因；
3. 如果合法，则执行返回 ACF（Admission Confirm）信息的步骤 604，



进行许可确认; 该 ACF 信息包含可信节点 120 的地址;

4. 终端 811 向可信节点 120 发起呼叫的步骤 605, 该呼叫信息中包含被呼叫节点即终端 821 的用户信息;
5. 可信节点 120 将有关信息发往网守 400 申请鉴权的步骤 606, 如果呼叫不合法, 则执行步骤 607, 返回 ARJ (Admission Reject) 信息, 该信息一般包含失败原因;
6. 如果呼叫合法, 可信节点 120 将实施呼叫被叫节点即终端 821 的步骤 608;
7. 如果终端 821 无应答, 则可信节点 120 向终端 811 执行步骤 609, 返回失败信息, 如果终端 821 应答, 则可信节点 120 实施步骤 610, 将该应答转发给主叫节点即终端 811, 实现呼叫的建立。

请一并参阅图 4、图 5 和图 7, 本发明网络安全方法具体的数据传送方式包括下述步骤:

1. 可信节点 120 转发终端 811 和 821 之间的能力交换和主从决定等信令, 由于信令通道选择单元 123 采用 Q931 通道传送信令, 使得所有的信令都通过 Q931 通道传送, 从而实现信令端口的收敛的步骤 701;
2. 主叫节点即终端 811 向可信节点 120 发出打开逻辑通道信令 (OLC), 该信令包含了关于传送数据的描述, 呼叫通道选择单元 124 选择特定的媒体流接收端口 129 的步骤 702, 一般情况下, 逻辑通道必须在终端 811 和 821 有能力同时接收所有打开通道的数据时才被打开;
3. 可信节点 120 将其 IP 地址和选定的媒体流接收端口 129 通知终端 811 的步骤 703, 由于对内部网络 810 中所有节点均采用同一媒体流接收端口 129, 从而可实现媒体流的收敛;
4. 可信节点 120 向终端 821 发送打开逻辑通道信令, 建立相应的通道的步骤 704, 所有外部网络 820 中的节点发出的码流经可信节点 120 后均由同一媒体流端口 129 转发至内部网络 810;
5. 可信节点 120 的数据转发单元 122 在控制单元 121 的控制下接收来自终端 811 和 821 的码流, 并转发给对应的终端 821 和 811, 实现视讯通信的步骤 705。



以上描述的是由内部网络810中的终端811向外部网络820中的终端821发起的视讯通信，终端821也可以向终端811发起呼叫。当然本发明还可以实现内部网络810中其他节点与外部网络820中其他节点之间的数据传送。

本发明还可以同时部署多个可信节点120，如果某个可信节点120达到带宽极限，则会向网守400报告资源不可用，网守400可将呼叫分配到另外的可信节点120上。实现负载均衡。扩展性非常好。

本发明由于引入可信节点120，则内部网络810的数据传送目的就只是可信节点，防火墙110可以做限制，即只有到可信节点810的通信才允许通过防火墙，增强网络安全性。由于所有内部节点与外部节点的视讯通信都先经过可信节点120。可信节点120与内部节点的信令和码流通信都实现收敛，从而避免了防火墙110过多端口的开发，也避免了码流的复用、解复用，从而基本不增加时延。

以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以作出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。



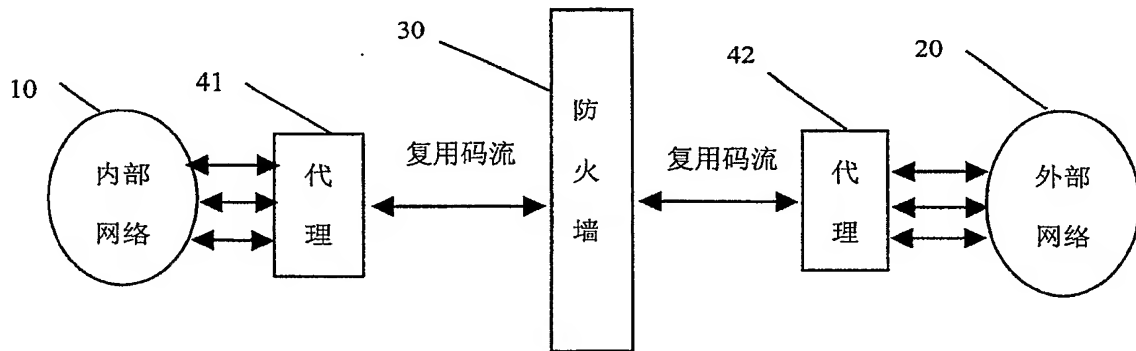


图 1

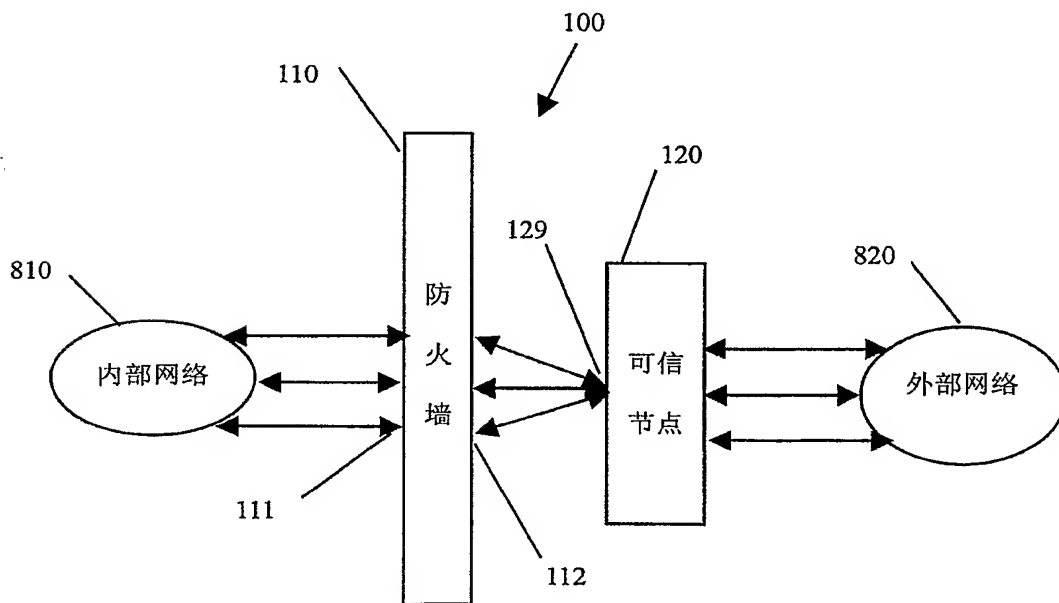


图 2



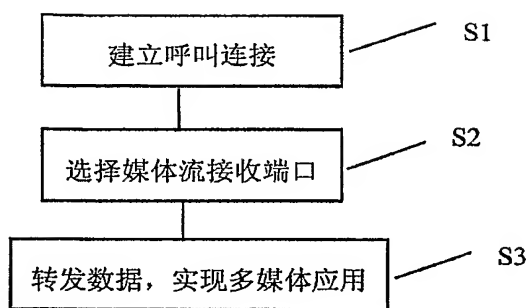


图 3

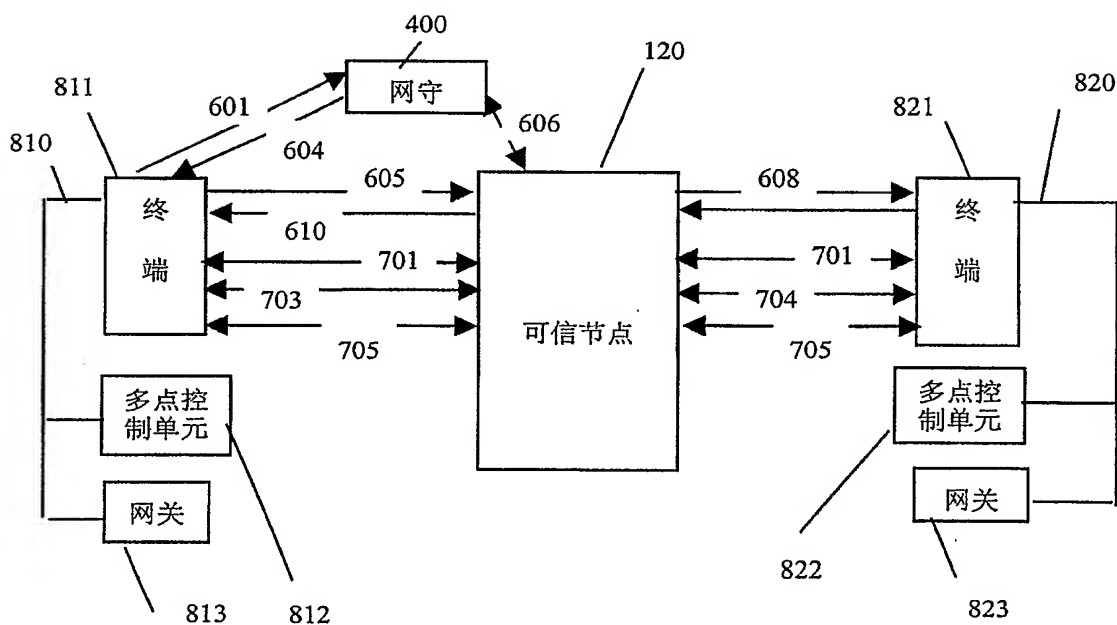


图 4



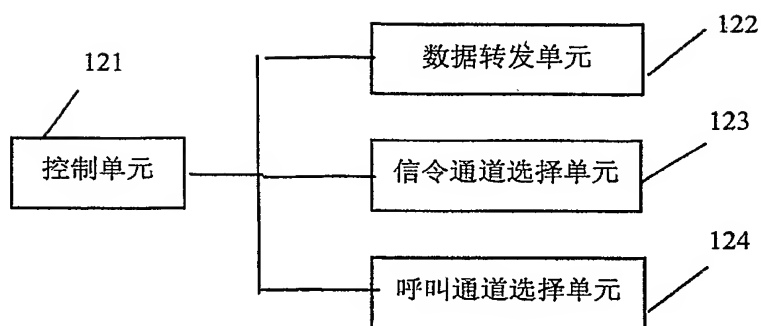


图5

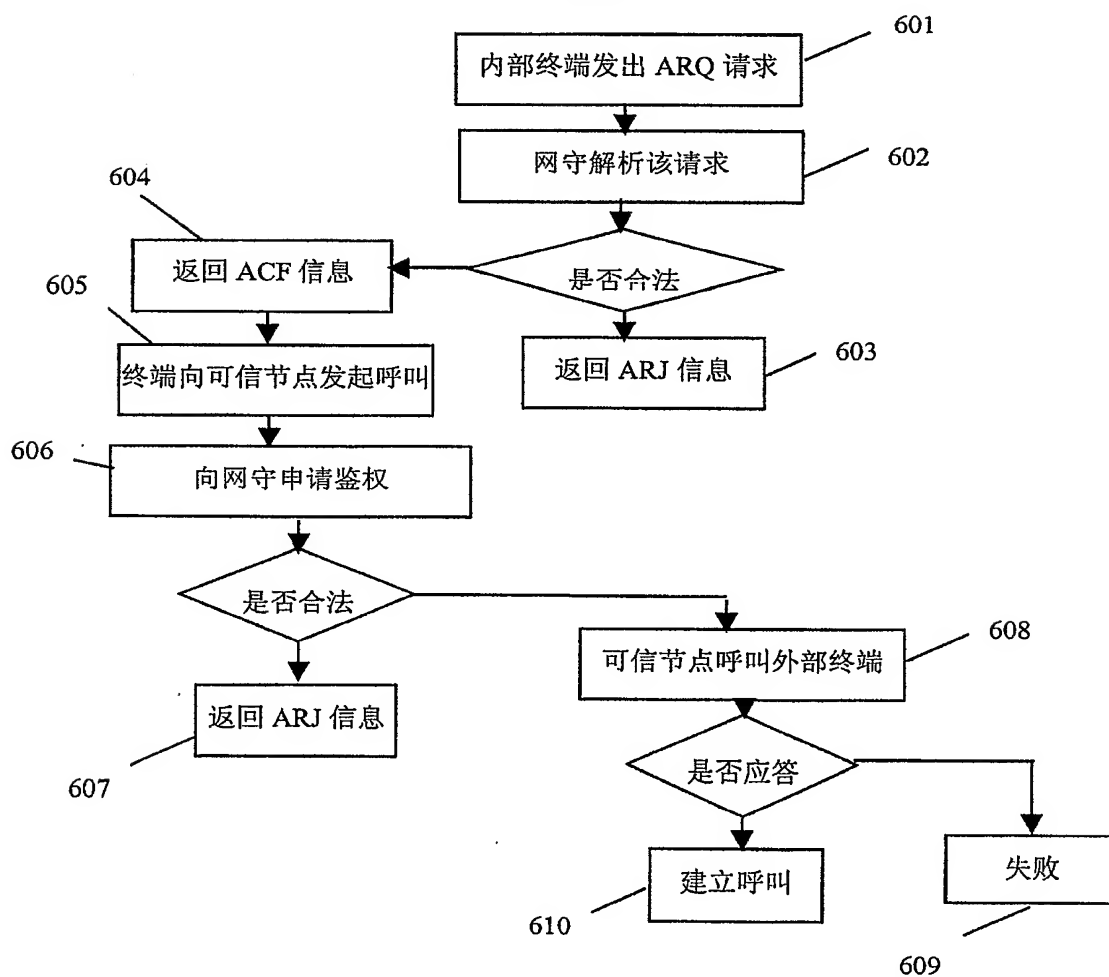


图6



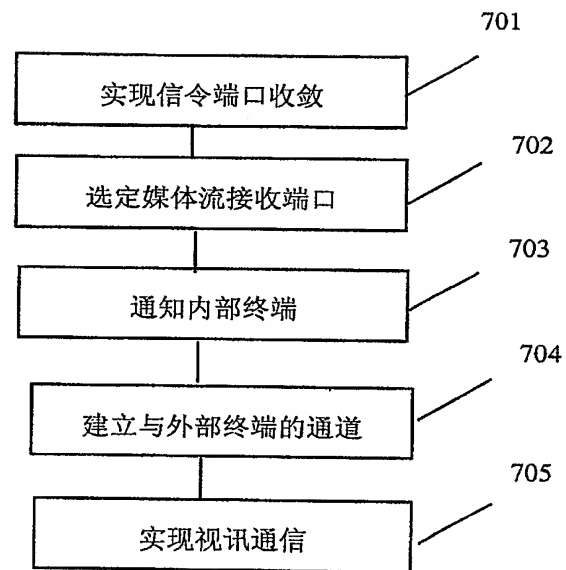


图 7

